

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff,	§	
	§	
VS.	§	Criminal No. 3:16-CR-306-D(1)
	§	
DARYL GLENN PAWLAK,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION  
AND ORDER

The instant motions to suppress and dismiss the indictment challenge the Federal Bureau of Investigation's ("FBI's") seizure of a computer server that hosted a child pornography website called "Playpen," and the FBI's ensuing operation of the website on a government server. Following a hearing, and for the reasons that follow, the court denies defendant Daryl Glenn Pawlak's ("Pawlak's") motions.<sup>1</sup>

I

The facts of this case that are material to the court's decision are undisputed.<sup>2</sup> In early

---

<sup>1</sup>Pursuant to Fed. R. Crim. P. 12(d), the court sets forth its essential findings in this memorandum opinion and order.

<sup>2</sup>The government intended to call FBI Special Agent Daniel Alfin ("Special Agent Alfin") to testify as to the network investigative technique ("NIT") warrant procedure. Pawlak planned to cross-examine Special Agent Alfin to establish that FBI agents acted with reckless disregard and conscious indifference for Rule 41. Due to illness, Special Agent Alfin was unable to attend the hearing. Pawlak moved for a continuance to ensure Agent Alfin's attendance. In denying the motion, the court stated that, if it determined Special Agent Alfin's testimony was necessary to decide the motion, it would reconvene the hearing. Because the court concludes that Special Agent Alfin's testimony is unnecessary for its

2015, acting on a tip from a foreign law enforcement agency, the FBI located and seized a computer server that contained a child pornography website called Playpen. Playpen existed as a hidden website on the Tor Network,<sup>3</sup> also known as the dark web. Through sophisticated encryption, the Tor Network anonymizes and actively conceals identifying information about website users, including a user's true Internet Protocol ("IP") address. To access Playpen, it was necessary for users to know the website's address on the Tor Network. Users could not, for example, stumble upon Playpen while browsing the Internet. Once on the Playpen website, users logged in with dedicated usernames and passwords. Playpen offered users various forums for different child pornography topics, including "Incest" and "Toddlers." Inside each forum were discussion posts, images, and videos related to the particular topic.

Because the Tor Network anonymizes its users, the FBI could not uncover who was operating or accessing the Playpen website through normal investigative techniques. The FBI devised a plan to investigate Playpen's users, who would normally be untraceable. The plan called for the FBI to copy the Playpen server and continue to operate the Playpen website on the FBI server. While operating the website, the FBI would use a network

---

analysis of the good-faith exception, it adheres to its decision declining to continue the hearing. And because Pawlak has not identified any other testimony that, if developed on direct or cross-examination, could alter the result and reasoning of the court's decision, it declines to continue the hearing for any other reason.

<sup>3</sup>"Tor" refers to The Onion Router, which was originally developed by an entity of the United States Government.

investigative technique (“NIT”) that allowed it to retrieve information from the computers of the persons who logged in to the Playpen website. The NIT—computer code developed by the FBI—would be attached to various files uploaded to Playpen. When the website user downloaded a file, the NIT would force the user’s computer to send to the FBI the user’s actual IP address and other identifying information. With the actual IP address, the FBI could identify and locate the user.

Acting according to the plan, the FBI copied the Playpen server and brought it to a government facility located in the Eastern District of Virginia. On February 20, 2015 the FBI applied for and obtained from a United States Magistrate Judge of the Eastern District of Virginia a search warrant (the “NIT Warrant”) authorizing the FBI to deploy the NIT program for a period of up to 30 days. The FBI also obtained from a United States District Judge a Title III order authorizing the FBI to intercept private messages and private chats in real time on the Playpen website. But the government acknowledges that Pawlak’s username did not engage in private messages or chats during the period of time the FBI monitored communications under the Title III order.

On or about March 4, 2015, Pawlak accessed the Internet from his residence using a laptop computer that his employer, Sigma Cubed, had issued. Using the Tor Network, he logged in to the Playpen website and clicked on a post entitled, “My daughter 5yo-photo 2015.” As the content from this post downloaded onto the laptop, the NIT computer code was sent automatically. The NIT relayed Pawlak’s IP address and other information back to the FBI in the Eastern District of Virginia.

Based on this information, the FBI issued a subpoena to AT&T, the Internet service provider connected with Pawlak's IP address, and learned that Pawlak's wife was the account holder associated with the address. The FBI obtained a warrant to search Pawlak's residence, but it did not find computers containing child pornography. While executing the warrant, agents called Pawlak's wife's cell phone, and Pawlak answered. He volunteered the details of how he accessed and viewed child pornography. Thereafter, the FBI contacted Pawlak's current employer, Independence Oil Field Chemicals, and his previous employer, Sigma Cubed, to request access to the work computers issued to him. The companies granted permission, and upon searching these computers, the FBI found hundreds of images of child pornography.

The grand jury later indicted Pawlak for the offenses of receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), and possession of child pornography involving a prepubescent minor, in violation of 18 U.S.C. § 2252A(a)(5)(B). Pawlak moves to suppress all information obtained by the NIT that was authorized pursuant to the application for Title III interception on or about February 20, 2015 in the Eastern District of Virginia and the application for the search of computers that access the Playpen website on or about February 20, 2015. He also moves to dismiss the indictment. The government opposes both motions.

## II

The court first considers Pawlak’s motion to suppress evidence that he alleges was collected in violation of the Fourth Amendment.<sup>4</sup>

The general rule under the Fourth Amendment is that searches of private property are reasonable if conducted pursuant to a valid warrant issued upon probable cause. *See, e.g., Katz v. United States*, 389 U.S. 347, 357 (1967). “A defendant normally bears the burden of proving by a preponderance of the evidence that the challenged search or seizure was unconstitutional.” *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005) (citing *United States v. Guerrero-Barajas*, 240 F.3d 428, 432 (5th Cir. 2001)). “The exclusionary rule prohibits introduction at trial of evidence obtained as the result of an illegal search or seizure.” *United States v. Runyan*, 275 F.3d 449, 466 (5th Cir. 2001). The exclusionary rule also “encompass[es] evidence that is the indirect product or ‘fruit’ of unlawful police conduct.” *Id.* (citing *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)).

## III

The court considers first the legality of the search. Pawlak contends that the search was unlawful because it exceeded the scope of the NIT Warrant. Pawlak maintains that the warrant “states that the property to be seized—the data including the identifiers from the Activating Computers—was . . . located in the Eastern District of Virginia,” and authorized

---

<sup>4</sup>The court assumes *arguendo* that Pawlak had a reasonable expectation of privacy in his work computer and that the NIT constituted a search that triggered the protections of the Fourth Amendment.

a search only of “one FBI computer server located in the Eastern District of Virginia hosting child pornography.” D. Br. 13-14. This is a mischaracterization of the NIT Warrant.

The NIT Warrant includes a standard court form that incorporates Attachments A and B. Although the form states that the property is located in the Eastern District of Virginia, it also specifically cites, and implicitly incorporates, Attachments A and B. Attachment A, entitled “Place to be Searched,” provides that the NIT warrant authorizes the use of an NIT to be deployed on the computer server described in Attachment A to obtain information described in Attachment B from the activating computers described in Attachment A. Attachment A identifies the computer server as “the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL [website redacted by the court] which will be located at a government facility in the Eastern District of Virginia.” Gov’t Br. Attach. A at 4. Attachment A identifies the “[t]he activating computers” as “those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.” *Id.* Attachment B, entitled “Information to be Seized,” provides that specific information is to be seized “[f]rom any ‘activating’ computer described in Attachment A.” Gov’t Br. Attach. B at 5. The NIT Warrant therefore authorizes the search and seizure of the server operating the Tor Network child pornography website, which is located at a government facility in the Eastern District of Virginia, and the activating computers, wherever located. It is not limited in scope to one FBI computer server located

in the Eastern District of Virginia.<sup>5</sup>

#### IV

Pawlak also challenges the validity of the NIT Warrant on the ground that it was an improper general warrant.

#### A

Under the Fourth Amendment, “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “Because indiscriminate searches and seizures conducted under the authority of ‘general warrants’ were the immediate evils that motivated the framing and adoption of the Fourth Amendment, that Amendment requires that the scope of every authorized search be particularly described.” *Walter v. United States*, 447 U.S. 649, 657 (1980) (internal quotation marks and citation omitted). “The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.” *Marron v. United States*, 275 U.S. 192, 196 (1927). In other words, the Fourth Amendment proscribes “issuance of general warrants allowing officials to burrow through a person’s possessions looking for any evidence of a crime.” *Kimbrough*, 69 F.3d at 727 (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). For example, in *United States v. Quinlan*, 1998 WL 414295, at \*1 (5th Cir. 1998) (per curiam) (unpublished

---

<sup>5</sup>The court does not suggest that this intent was a valid exercise of the magistrate judge’s authority. *See infra* § V(B).

table decision), the panel held that a warrant was general where it authorized seizure of “property that constitutes evidence of the commission of a criminal offense and/or contraband, the fruits of a crime, and/or things criminally possessed.” *Id.* at \*1.

Pawlak contends that the NIT Warrant was a general warrant because it “did not specify or identify any particular Activating Computer or router/modem the Government wished to search.” D. Br. 15. The NIT Warrant identified the “Place to be Searched” as the computer server operating the Tor network child pornography website, to be located at a government facility in the Eastern District of Virginia, and “activating computers,” that is, computers “of any user or administrator who logs into the [Playpen website] by entering a username and password.” Gov’t Br. Attach. A at 4. Under the heading “Information to be Seized,” the NIT Warrant authorized the seizure of seven specific categories of information, including “the ‘activating’ computer’s actual IP address.” *Id.* at 5.

## B

The court concludes that the NIT Warrant was not a general warrant. The NIT Warrant limited the search to only the host server for the Playpen website, to be located at a government facility in the Eastern District of Virginia, and to defined “activating computers,” that is, computers “of any user or administrator who logs into [the Playpen website] by entering a username and password.” Gov’t Br. Attach. A at 4. Because the magistrate judge found that the information to be seized from the server and activating computers would be evidence of multiple violations of federal child pornography laws, the warrant was not broader than necessary to uncover evidence of criminal activity. *See, e.g.,*



*United States v. Matish*, 193 F.Supp.3d 585, 609 (E.D. Va. 2016) (“[T]here existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography.”).

V

Pawlak also contends that the magistrate judge who issued the NIT Warrant lacked authority under both Fed. R. Crim. P. 41(b) (2015)<sup>6</sup> and § 636(a) of the Federal Magistrate Judges Act, 28 U.S.C. § 636(a),<sup>7</sup> to authorize the search of a computer in Texas.

---

<sup>6</sup>Amended Rule 41(b)(6), which took effect on December 1, 2016, remedies the limitation on the magistrate authority that is discussed in this and several other decisions related to the NIT Warrant. It provides:

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The parties agree that this new rule is inapplicable in this case.

<sup>7</sup>Relevant here, § 636(a) provides that magistrate judges shall have “within the district . . . all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts.”

A

Pawlak contends that the magistrate judge in the Eastern District of Virginia lacked authority under Rule 41 to authorize the search of a computer in Texas. The government responds that the NIT is functionally a tracking device that “was used to track the movement of information both within and outside of Virginia.” Gov’t Br. 21. According to the government, “[t]he NIT program, by way of operation, used [a communication stream between the government’s server in Virginia and Pawlak’s computer in Texas] to track from where the computer signal emanated.” *Id.* at 22.

B

Rule 41(b)(4) provides that “a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.” A “tracking device” is “an electronic . . . device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117; *see also* Rule 41(a)(2)(E) (incorporating definition in § 3117). And the rules indicate that “property” includes “information.” Rule 41(a)(2)(A).

The courts that have considered the NIT Warrant have split on the issue. *See United States v. Torres*, 2016 WL 491223, at \*4 (W.D. Tex. Sept. 9, 2016) (collecting cases). Courts that have held that Rule 41(b) was not violated have concluded that the defendants “voluntarily and deliberately came to the Eastern District of Virginia when [they] took affirmative steps to log into the Playpen website by entering a username and password.”

*United States v. Sullivan*, 2017 WL 201332, at \*6 (N.D. Ohio Jan. 18, 2017); *see also United States v. Anzalone*, \_\_\_ F.Supp.3d \_\_\_, 2016 WL 5339723, at \*9 (D. Mass. 2016) (collecting cases). It was therefore permissible for the magistrate judge to authorize affixing a tracking device—i.e., the NIT code—to the defendants’ computers once they were present in the district. Courts that have held that the magistrate judge violated Rule 41(b) have reasoned that the government’s defense of the magistrate judge’s authority stretches the Rule. *See, e.g., United States v. Hammond*, \_\_\_ F.Supp.3d \_\_\_, 2016 WL 7157762, at \*4 (N.D. Cal. Dec. 8, 2016) (“[Defendant’s] computer is a physical object that at all times remained in his home in the Northern District of California, and the download, too, occurred here and not ‘virtually’ in the Eastern District of Virginia.”).

The court agrees with the courts that have concluded that Rule 41(b)(4) does not extend to the NIT Warrant. Although caselaw suggests that the court is to construe Rule 41(b) broadly, *see United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977) (holding that Rule 41(b) “is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause”), it cannot render it meaningless. As one court has explained:

[i]f the “installation” occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [defendant’s] computer, applying the tracking device exception again fails, because [defendant’s] computer was never physically located within the Eastern District of Virginia.

*United States v. Michaud*, 2016 WL 337263, at \*6 (W.D. Wash. Jan. 28, 2016).

Accordingly, the court holds that the NIT Warrant exceeded the magistrate judge's authority under Rule 41(b) by authorizing the search of a computer in Texas.

C

Although the NIT Warrant violated Rule 41(b), it does not follow automatically that the search and seizure in this case should be suppressed.

1

The exclusionary rule precludes the government from relying on illegally-seized evidence. *United States v. Houltin*, 566 F.2d 1027, 1030 (5th Cir. 1978). “The purpose of the exclusionary rule is to deter unlawful police conduct.” *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006). This purpose will not be served, and thus the rule is inapplicable, where evidence is obtained in “objectively reasonable good-faith reliance upon a search warrant.” *Id.* (citations and internal quotation marks omitted). “Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers’ reliance on the warrant was objectively reasonable and in good faith.” *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003) (citing *United States v. Leon*, 468 U.S. 897, 921-25 (1984)). The good-faith exception cannot apply if “the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth[.]” *Id.* at 399 (quoting *United States v. Webster*, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992) (per curiam)). “The ‘good faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the

search was illegal despite the magistrate's authorization.” *Pope*, 467 F.3d at 917 (quoting *Leon*, 468 U.S. at 922 n.23).

In the context of a Rule 41 violation,

where there is no constitutional violation nor prejudice in the sense that the search would likely not have occurred or been as abrasive or intrusive had Rule 41 been followed, suppression . . . is not appropriate if the officers concerned acted in the affirmative good faith belief that the warrant was valid and authorized their conduct.

*United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986). This is because the balance of interests inherent in an exclusionary rule analysis “weighs much less heavily [when] the [Rule 41] violation is neither of constitutional dimensions nor intentional.” *Id.* at 1210.

2

Pawlak maintains that, as a threshold matter, the good-faith exception cannot apply where a warrant was void at its outset. *See United States v. Levin*, 186 F.Supp.3d 26, 38-42 (D. Mass. 2016) (holding that good-faith exception is inapplicable to NIT because NIT Warrant was void *ab initio*). The court is unaware of any binding precedent in this circuit that restricts the exception in this manner, and it therefore declines to adopt this rule.<sup>8</sup>

3

The court must also evaluate whether the Rule 41(b) violation prejudiced Pawlak by subjecting him to a search that would not have occurred or that would have been less

---

<sup>8</sup>The Sixth Circuit once followed this rule, but later abandoned it because it was “no longer clearly consistent with current Supreme Court doctrine[.]” *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010).

intrusive absent the violation. *See Comstock*, 805 F.2d at 1207. Pawlak contends he suffered prejudice because he would not have been subjected to the search absent the Rule 41(b) violation. The court disagrees.

The version of Rule 41(b) in effect on February 20, 2015 would not have permitted a magistrate judge of the Eastern District of Virginia to issue the NIT Warrant. *See supra* § V(B). But it would not have precluded a district judge in that district from issuing the same warrant. *United States v. Jean*, \_\_\_ F.Supp.3d \_\_\_, 2016 WL 4771096, at \*12 n.16 (W.D. Ark. Sept. 13, 2016) (“District judges are not limited by Rule 41(b) as magistrate judges are. Instead, district judges may issue warrants to search property located outside their judicial districts when the requirements of the Fourth Amendment are met.”). Pawlak does not contend that the NIT Warrant is not supported by probable cause. Accordingly, had a district judge been presented the same warrant application, the district judge would have been authorized to issue a warrant for the search of Pawlak’s computer in Texas. The court therefore concludes that the Rule 41(b) violation was technical.

4

The final aspect of the court’s analysis is whether law enforcement acted with an intentional disregard of Rule 41(b). Pawlak contends that the good-faith exception is inapplicable because the government willfully violated Rule 41(b), 41(F)(1)(C), 41(F)(1)(B), and 41(F)(1)(D).

Pawlak first contends that the FBI agents responsible for securing the NIT Warrant either were or should have been well aware that it violated Rule 41(b). Pawlak points to

circumstantial evidence, including allegations of forum-shopping, to illustrate that the government's violations were intentional. Regardless of the agents' subjective beliefs, however, it was far from clear at the time that the NIT Warrant violated Rule 41(b). In fact, several courts have held that the NIT Warrant did *not* violate Rule 41(b). *See, e.g., Jean*, 2016 WL 4771096, at \*16-17. Accordingly, although this court has held that the NIT warrant violated Rule 41(b) by exceeding the magistrate judge's authority, the court also concludes that the government did not intentionally violate the Rule.

Pawlak also contends that the government willfully violated Rule 41(f)(1)(C) because it did not give him timely notification of the NIT Warrant, as the Rule requires. But the magistrate judge extended the notification deadline three times, as permitted by Rule 41(f)(3), so that notification was not required until March 20, 2016. The lead case agent on the investigation averred in a declaration that she emailed redacted copies of the NIT Warrant to Pawlak's counsel on March 15, 2016. Accordingly, the court concludes that the government satisfied the requirements of Rule 41(f)(1)(C).

Finally, Pawlak contends that the government's return of the property to the issuing magistrate judge, as required by Rule 41(f)(1)(D), was deficient because the inventory included with the return did not comply with Rule 41(f)(1)(B).

Under Rule 41(f)(1)(B), "[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied." The return states that the inventory seized from the NIT was "Data from computers that accessed TARGET

WEBSITE between 2/20/15 and 3/4/15.” Gov’t Br. Attach. A at 40. Pawlak contends this is insufficient because “[t]here is no indication which devices or computers were searched, how many computers were searched,” and other relevant information. D. Br. 32. The court disagrees. Rule 41(f)(1)(B) does not require the detail that Pawlak demands. And here, there is no physical storage media to describe; the FBI seized data transmitted to the host server from the activating computers.

Accordingly, the court concludes, as has nearly every other court to consider this question, that the good-faith exception applies to the execution of the NIT Warrant. *See, e.g., Anzalone*, 2016 WL 5339723, at \*10. The court therefore denies the motion to suppress.

## VI

The court now considers Pawlak’s motion to dismiss the indictment. Pawlak contends that the government’s control and maintenance of the Playpen website was so outrageous as to constitute a due process violation under the Fifth Amendment.

## A

The Supreme Court has contemplated that it “may some day be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction[.]” *United States v. Russell*, 411 U.S. 423, 431-32 (1973). The conduct that is so outrageous as to warrant dismissal is undeveloped in the caselaw. The Fifth Circuit in *United States v. Tobias*, 662 F.2d 381, 386 (5th Cir. Unit B Nov. 1981), provided a broad framework. In *Tobias* the court affirmed the denial of dismissal where the government agent,



posing as a chemical supplier, convinced the defendant to manufacture Phencyclidine and agreed to send the defendant “everything he needed to get set up.” *Id.* at 383-84. Although the Fifth Circuit concluded that this was a permissible infiltration of criminal activity as a means of investigation, it noted that the government cannot “instigate the criminal activity, provide the place, equipment, supplies and know-how, and run the entire operation with only meager assistance from the defendants without violating fundamental fairness.” *Id.* at 386.

## B

Pawlak maintains that the government’s operation of the Playpen website crossed this outer limit set by *Tobias*. He posits that the government instigated the activity by relaunching the Playpen website from its own server in Virginia, and thereafter “provided the virtual place, equipment, and supplies for child pornography to be viewed, downloaded, and shared” with its maintenance of the website. D. Mot. to Dis. Br. 4. Pawlak contends that the government essentially ran the entire criminal enterprise, with defendants like Pawlak playing a small role.

The court disagrees with Pawlak’s argument, as has every other district court that has considered it. *See, e.g., United States v. Tran*, \_\_\_ F.Supp.3d \_\_\_, 2016 WL 7468005, at \*3 (D. Mass. 2016) (“Every district court to consider this same argument has found it wanting.”). It is undisputed that the government did not create the Playpen website. It did not alter the site’s functionality, add additional child pornography, or actively solicit new users. Rather, the government simply maintained the preexisting structure that Playpen website visitors allegedly used to distribute and receive child pornography among

themselves.

Moreover, Pawlak cannot maintain that he provided only “meager assistance” to the government. *See Tobias*, 662 F.2d at 386. The government has submitted evidence that shows that Pawlak opened his Playpen account in September 2014, long before the government took control of the website. And in order to activate the NIT, Pawlak must have sought out and downloaded specific images of child pornography from the Playpen website. This is more than meager assistance; it is active participation.


Accordingly, because Pawlak cannot show that the government violated his due process rights, the court denies his motion to dismiss.

\* \* \*

For the reasons explained, the court denies Pawlak’s motion to suppress and his motion to dismiss.

**SO ORDERED.**

February 17, 2017.

  
SIDNEY A. FITZWATER  
UNITED STATES DISTRICT JUDGE